FROM IDENTIFIER TO INTRUSION: THE LEGAL COMPLEXITY OF IP-ADDRESS-BASED INVESTIGATIONS

Miulescu Maria
Transilvania University of Braşov, Faculty of Law
Advanced Criminal Sciences Master
Year of study: 1st

Abstract

Modern IP addresses serve as critical digital identifiers that provide an intimate gateway into an individual's private life, uncovering personal habits, interests, and movements. Landmark jurisprudence, such as R. v. Bykovets in Canada and Breyer v. Germany in Europe, has recognized that these identifiers warrant significant constitutional protection because they allow for precise re-identification when correlated with third-party data. These rulings emphasize that an IP address is not merely a neutral technical string but a fundamental link in the chain of digital privacy.
However, a significant accountability gap persists as private third-party actors, such as ISPs, hold vast amounts of metadata that often fall outside the direct scope of constitutional scrutiny. This creates a paradox where law enforcement can indirectly obtain sensitive biographical information without the procedural guarantees required for direct state action. Consequently, legal frameworks must evolve toward more technologically informed standards that recognize the intrinsic sensitivity of IP-address-based information to prevent the normalization of digital intrusion.

INTRODUCTION

In the digital age, every individual leaves behind a continuous stream of online traces, ranging from website visits to online payments and communication metadata. Among these digital identifiers, the IP address has become a pivotal investigative tool for law enforcement agencies. Evidently, the emergence of new technological environments has also created opportunities for new forms of criminal activity. Yet this same technological expansion has increased the ability for authorities and private actors to monitor, track, and analyse individuals' online behaviour in unprecedented ways.

The act of identifying a person through their IP address therefore raises questions regarding the protection of fundamental rights, revealing concerns between constitutional ideals and the realities of contemporary digital investigations. Although often perceived as merely a string of abstract numbers, the IP address is an entry point into a person's private digital life, uncovering their habits, interests, movements, and interactions. This transforms what might appear as a routine procedural formality into a potential source of personal intrusion.

Thus, this essay demonstrates how IP-address-based investigations and online surveillance challenge privacy and data protection. Ultimately, this highlights the need for legal frameworks to adapt so that constitutional guarantees remain fully protected amid rapid technological change. The following analysis will examine the technical foundations of IP-address-based identification, the privacy challenges illustrated through key jurisprudence in Canada and Europe, as well as the effectiveness of existing legal frameworks in addressing these risks.

1. DIGITAL PRIVACY FOUNDATIONS

1.1. Reasonable expectation of privacy

Firstly, with the rise of technology, an Internet user should not feel obliged to abandon online activities altogether in order to preserve their privacy. This creates a paradox between the desire for confidentiality and the demands of digital infrastructure, where mere participation involves a partial loss of control over personal data. As a result, information shared can be exploited by third parties for commercial, security or legal reasons, reducing user's ability to manage or limit access to their biographical information in today's digital environment.

To mitigate this issue, the notion of reasonable expectation of privacy plays a central role. In Canada, as affirmed in *Bykovets*, this concept refers to the fact that individuals can expect that their personal information, communications, and behaviours will remain protected by the state and third-party actors. This expectation is evaluated objectively, and englobes what society deems as a legitimate claim to privacy in given circumstances. Nonetheless, the private nature of the information that an IP address can uncover strongly suggests that the public's reasonable expectation of privacy should outweigh the government's interest in achieving its investigative objectives.

One could argue that this standard is specific to Canadian jurisprudence and therefore not universally applicable. However, in Europe, the right to privacy is not only formalised by art. 8 of the ECHR, but also a "threshold test"[1] designed to better protect the average user[2]. For example, when a person orders a product online, they can reasonably expect that the service

[1] BPP Human Rights Unit. *Article 8 and the "reasonable expectation of privacy test."* BPP Human Rights Law Blog, 2021, available at: https://bpphumanrightsunit.wordpress.com/2021/02/24/article-8-and-the-reasonable-expectation-of privacy-test/, accessed on 02.12.2025, at 14:05.
[2] BPP Human Rights Unit. *Article 8 and the "reasonable expectation of privacy test."* BPP Human Rights Law Blog, 2021, available at: https://bpphumanrightsunit.wordpress.com/2021/02/24/article-8-and-the-reasonable-expectation-of privacy-test/, accessed on 02.12.202, at 14:10

provider will process their personal data solely for the purpose of fulfilling the transaction[3]. These measures are meant to consider how a reasonable person of ordinary sensibilities would feel if placed in the same position as the claimant, thereby ensuring that privacy expectations remain grounded in societal norms[4].

1.2. Essential context for Internet usage

Firstly, one can state that the social context of the Internet is essential to explaining the privacy interest that the Charter has regarding the information that an IP address can reveal[5]. Evidently, the architecture of the Internet has created a vast, accurate, and ever-expanding record of user activity that is "unprecedented in our society"[6]. More importantly, the very infrastructure of the Internet relies on the exchange of information to provide and access

services[7]. Rapid technological change makes it difficult to establish a precise definition of the Internet[8]. This is problematic for police investigations because they require a narrow and clear interpretation in order to act in accordance with the rights guaranteed by the Charter[9].

Indeed, factors such as the number of activities and individuals that may be affected, reasonable expectations of privacy, the significance of digital spaces for freedom of expression, and whether police investigative methods are sufficiently limited compared to other measures are weighed in determining the boundaries of these spaces. In other words, digital spaces are inherently dynamic, requiring a careful definition of the space targeted in a police investigation and a consideration of interactivity, among other factors.

Certain online spaces, such as search engines, allow users to explore things that they would not necessarily discuss in public. A contemporary example is social media, which allows

[3] Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 8; Kamara, I., & De Hert, P. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*. Brussels Privacy Hub Working Paper, Vol. 4, No.12 (Brussels, 2018), available at: https://www.brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf, p. 17, accessed on 08.12.2025, at 16:45.
[4] BPP Human Rights Unit. *Article 8 and the "reasonable expectation of privacy test."* BPP Human Rights Law Blog, 2021, available at: https://bpphumanrightsunit.wordpress.com/2021/02/24/article-8-and-the-reasonable-expectation-of privacy-test/, accessed on 08.12.2025, at 17:20.
[5] *R.* v. *Bykovets*, 2024 SCC 6, p 5
[6] *R.* v. *Bykovets*, 2024 SCC 6, p 50; *R.* v. *Vu*, 2013 SCC 60, p 40; A. D. Gold, « Applying Section 8 in Digital World: Seizures and Searches », document préparé pour le 7th Annual Six-Minute Criminal Lawyer (9 juin 2007), p 3.
[7] *R.* v. *Ramelson*, 2022 SCC 44, p 44.
[8] *R.* v. *Ramelson*, 2022 SCC 44, p 42.
[9] *R.* v. *Ahmad*, 2020 SCC 11, p 43.

individuals to hide behind a façade of their choosing. This signifies that biographical information can be more easily revealed when using the Internet, thus precisely identifying people[10].

Finally, the broad context of the Internet should not be interpreted as a justification for systemically eroding privacy rights. Even in an environment where information sharing is inevitable for accessing services, limits must be set to respect user's privacy. The Internet plays a crucial role in everyday life, whether it be for shopping, paying bills, conducting research, or even communicating with loved ones. Protecting privacy should not require users to fully refrain from engaging in these daily online activities.

1.3. Informational intimacy modified by the Internet

Secondly, the topography of informational intimacy depicts how IP addresses, or so-called digital breadcrumbs, have become central to mapping a person's intimate online life, especially when combined with data collected by third-party corporations.[11] An IP address is a unique identifier for a device on a network, but it can also uncover geographical location and the ISP. When correlated with other online activity, it can be utilized to build a detailed profile of a person's interests and behaviours, raising substantial privacy concerns.[12]

1.3.1. IP addresses as personal data

At first glance, an IP address may appear to be merely a string of numbers with no inherent meaning. While individuals across the globe may know it exists, they often do not realize what it stands for and how revealing it can be. Evidently, the European Court of Justice declared that IP addresses collected by the ISP are personal data[13]. This signifies that they enable accurate user identification[14]. According to art. 4(1) of the GDPR, an IP address is considered personal data because it is an online identifier that can leave traces used to create a profile and identify an individual, especially when combined with additional information collected by servers and third parties[15].

[10] Brennan, D. *CJEU rules IP addresses may constitute personal data*. A&L Goodbody, 2016, available at: https://www.algoodbody.com/insights-publications/cjeu-rules-ip-addresses-may-constitute-personal-data, p.1, accessed on 08.12.2025, at 17:50.
[11] *R.* v. *Bykovets*, 2024 SCC 6, p 9.
[12] *R.* v. *Bykovets*, 2024 SCC 6, p 76.
[13] Đukanović, J. *Is IP address personal data*, Zunic Law, Serbia, 2025, available at: https://zuniclaw.com/en/ip-address personal-data/, accessed on 08.12.2025, at 18:38.
[14] Đukanović, J. *Is IP address personal data*, Zunic Law, Serbia, 2025, available at: https://zuniclaw.com/en/ip-address personal-data/, accessed on 08.12.2025, at 19:20.
[15] Regulation (EU) 2016/679 (General Data Protection Regulation), art. 4 (1).

Additionally, according to *Breyer*, an IP address can be dynamic, which means that although it does not directly reveal a person's identity, when correlated with data held by a third party, such as an ISP, it becomes identifiable[16]. Evidently, the ISP logs which customer had a given IP address at a given time, thereby transforming it into a key that allows re identification[17].

1.3.2. Information disclosed to ISPs

Due to the structure of the Internet, third-parties, such as ISPs, web search engines, and social media platforms, now have the ability to analyse user's data. In fact, an ISP necessarily knows a user's IP address, since it is the one assigning it. This means the ISP can directly link the address to the user's identity, including their name and billing information, since obtaining a unique IP address requires a contractual and paid service. As a result, an ISP is technically capable of logging and reconstructing a user's online activities if it chooses to do so.

That being said, many online activities can be encrypted through the HTTPS, which protects the content of communications[18]. Under the former HTTP, ISPs and other intermediaries could intercept and store unencrypted browsing data[19]. However, the ISP can still access important metadata through the HTTPS, such as the websites visited, as well as other connection-related information like Amazon[20].

Since these same parties are not subject to the same constitutional protections as the State, they could use one's data and make inferences about sensitive aspects of a user's lifestyle, such as habits, interests and behaviours[21]. Moreover, when faced with a court order or warrant, an ISP must disclose identifying information, such as a subscriber's name and address, if the police asserts that activities linked to an IP address are unlawful.

[16] *Breyer* v. *Germany*, 2020, 50001/12, p 4.
[17] Breyer v. Germany, 2020, 50001/12, p 4.
[18] Amazon Web Services, Inc., « What's the Difference Between HTTP et HTTPS? », 2024, available at: https://aws.amazon.com/compare/the-difference-between-https-and-http/, accessed on 09.12.2025, at 20:50.
[19] Amazon Web Services, Inc., « What's the Difference Between HTTP et HTTPS? », 2024, available at: https://aws.amazon.com/compare/the-difference-between-https-and-http/, accessed on 09.12.2025, at 21:20.
[20] Amazon Web Services, Inc., « What's the Difference Between HTTP et HTTPS? », 2024, available at: https://aws.amazon.com/compare/the-difference-between-https-and-http/, accessed on 09.12.2025, at 21:46.
[21] *R.* v. *Bykovets*, 2024 SCC 6, p 73.

2. CHALLENGES TO PRIVACY IN ONLINE INVESTIGATIONS

2.1. Canadian jurisprudence: *R.* v. *Bykovets*

Firstly, given the technical nature surrounding the notion of reasonable expectation of privacy, the IP addresses, the topography of informational intimacy, and ISPs, it is essential to anchor the discussion in established jurisprudence. The jurisprudence exemplified by *Bykovets* provides a valuable framework to understand how these technical issues intersect with legal principles.

This case raises the question of whether an IP address gives rise to a reasonable expectation of privacy, such that a police request to obtain it constitutes a search within the meaning of art. 8 of the Charter[22].

In September 2017, the Calgary Police Service investigated fraudulent online purchases from a liquor store, with payments processed by Moneris, a third-party payment processor[23].The police requested the IP addresses associated with these transactions from Moneris, and two addresses were provided[24]. Through a judicial production order, the police then compelled the ISP to disclose the names and addresses of the customers associated with these IP addresses, one of which was registered to the appellant[25]. This information led the police to execute a search warrant at the appellant's residence, resulting in his arrest for offenses related to fraudulent use of credit cards and identities[26].

The appellant challenged the disclosure of his IP address prior to trial, claiming an infringement of his right to privacy under art. 8 of the Charter[27]. He argued that the request for his IP address constituted a "search" because he had a reasonable expectation of privacy regarding this information[28]. The majority of the Supreme Court of Canada held that the IP address was the essential link between the appellant and his online activity and that it warranted protection sufficient to guarantee his reasonable expectation of privacy. Accordingly, a police request to obtain the IP address constituted a search within art. 8 of the Charter[29]. The Court

[22] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982 [Schedule B to the Canada Act 1982, 1982, c. 11 (U.K.)], art. 8
[23] *R.* v. *Bykovets*, 2024 SCC 6, p 97.
[24] *R.* v. *Bykovets*, 2024 SCC 6, p 98.
[25] *R.* v. *Bykovets*, 2024 SCC 6, p 98.
[26] *R.* v. *Bykovets*, 2024 SCC 6, p 99.
[27] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982 [Schedule B to the Canada Act 1982, 1982, c. 11 (U.K.)], art. 8; *R.* v. *Bykovets*, 2024 SCC 6, p 100.
[28] *R.* v. *Bykovets*, 2024 SCC 6, p 100.
[29] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982 [Schedule B to the Canada Act 1982, 1982, c. 11 (U.K.)], art. 8.

therefore allowed the appeal, set aside the convictions, and ordered a new trial[30].

This jurisprudence illustrates why IP-address-based investigations present significant legal and constitutional challenges. Although an IP address may appear to be a neutral technical identifier, it functions as a gateway to an individual's online activities, enabling authorities to reconstruct patterns of behaviour, personal interests, and other intimate details. This decision shows that obtaining an IP address is not merely a routine investigative step, but the first link in a chain that can ultimately identify a person with precision once correlated with ISP data. Ultimately, these links within the digital ecosystem creates a risk of excessive state surveillance, particularly because IP addresses are generated automatically, collected, and often retained without the user's knowledge or consent. Moreover, it demonstrates how blurred and conceptually unstable the boundary is between seemingly harmless metadata and information that intrudes upon core privacy interests. Finally, this ambiguity poses a risk because investigative practices may appear simple and reasonable, but in reality, they encourage forms of state surveillance that bypass constitutional protections.

2.2. European jurisprudence: Breyer v. Germany

Secondly, the concerns highlighted in *Bykovets* are not unique to Canada as they reflect a broader international struggle to regulate how digital identifiers can be used in criminal investigations without eroding fundamental privacy rights. Similar tensions have emerged in Europe, where courts have likewise confronted the question of whether seemingly technical data, such as dynamic IP addresses, should be treated as personal information warranting constitutional protection. The European jurisprudence, particularly the *Breyer* case, offers a compelling perspective. It illustrates how the capacity to link IP addresses with third-party subscriber data transforms these identifiers into useful tools for state surveillance, thereby necessitating strict measures under data-protection and human-rights laws. Examining this parallel emphasizes the global nature of the challenges posed by IP-address-based investigations and the need for coherent privacy protections across jurisdictions.

In this instance, the applicants accessed several publicly accessible websites run by German federal institutions using prepaid mobile phone SIM cards[31]. Every time they connected, their dynamically assigned IP address was logged, along with other connection data,

[30] *R.* v. *Bykovets*, 2024 SCC 6, p 92.
[31] *Breyer* v. *Germany*, 2020, 50001/12, p 3.

by the website operator[32]. The State gained access to stored lists of IP addresses linked to access logs through the ISPs. Under section 111 of the Telecommunications Act, now amended, the Federal Constitutional Court claimed this storage was lawful because it protected against cyberattacks, ensured site functionality, and could potentially enable prosecution of attackers[33]. The applicants challenged this practice, arguing it violated art. 8 and art. 10 of the ECHR[34].

In the end, the *Breyer* judgment found a violation of art. 8 of the ECHR[35]. The interference was not proportionate, as no serious crimes were committed and there was no pressing social need to justify the investigation[36]. It clarified that dynamic IP addresses, although not directly identifying, constitute personal data when the website operator has legal means enabling the user's identification through an ISP[37]. By recognizing that identifiability relies not on what data reveals in isolation, but on what it can reasonably reveal once combined with third-party information, the Court reaffirmed a broad and protective interpretation of data privacy right[38]. The decision reinforced the notion that the State and private actors must treat IP-address-based investigations and logging practices as constitutionally sensitive activities subject to data-protection norms and proportionality requirements.

To conclude this chapter, both these jurisprudential cases reveal that the challenges posed by IP-address-based investigations stem from the very architecture of the Internet, not solely from investigative practices. This emphasizes the need for clear and coherent legal standards. The next section therefore turns to the existing legal frameworks in Canada and Europe to assess how they regulate these investigative techniques and whether they provide adequate protection for digital privacy.

3. LEGAL FRAMEWORKS IN CANADA AND EUROPE

3.1. Privacy and data protection in Canada

Building on the challenges raised in *Bykovets*, it is crucial to examine the legal frameworks that guarantee privacy and cybersecurity in IP-address-based investigations. These

[32] *Breyer* v. *Germany*, 2020, 50001/12, p 4.
[33] *Breyer* v. *Germany*, 2020, 50001/12, p 15 and 27.
[34] *Breyer* v. *Germany*, 2020, 50001/12, p 59; Charter of Fundamental Rights of the European Union (2000/C364/01), art. 8, art. 10.
[35] Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 8.
[36] *Breyer* v. *Germany*, 2020, 50001/12, p 26.
[37] *Breyer* v. *Germany*, 2020, 50001/12, p 5.
[38] *Breyer* v. *Germany*, 2020, 50001/12, p 20.

frameworks must reconcile the evolving nature of digital surveillance with constitutional rights.

Under art. 8 of the Charter, individuals are protected against unreasonable search and seizure, while p 24(2) allows courts to exclude evidence that would bring the administration of justice into disrepute[39]. In *R.* v. *Grant*, 2009 SCC 32, the Supreme Court of Canada formulated a three-part test to assess when exclusion is warranted, such as the seriousness of the state's breach, its impact on the rights of the accused, as well as the society's interest in trials on their merits[40].

Additionally, the *R.* v. *Spencer*, 2014 SCC 43 firmly establishes that IP addresses constitute personal information and that individuals have a reasonable expectation of privacy.[41] The Supreme Court held that the chain of disclosure from an ISP to the police constitutes a search under art. 8 of the Charter, highlighting the gap created when private actors hold critical data beyond the reach of constitutional protections[42]. This is why a warrant is required under art. 487 of the Criminal Code[43]. Moreover, per art. 487.1 of the Criminal Code, one could request a tele warrant, another reason why such a step does not impair the ability of law enforcement to investigate a crime[44]. When such a warrant is requested, the justice of the peace must balance the individual's privacy interests against the State's interest in conducting criminal investigations. The applicant must provide detailed information, and establish that what is sought out is likely evidence of an offence. In this instance, a *Spencer*-type warrant is not sufficient due to the sensitive nature of digital information and its unique position within the legal system.

This concern is further complicated by the rise of the Internet and the emergence of third-party actors, which has reshaped the topography of informational intimacy protected by the Charter. In *Bykovets*, Moneris, a private third-party company, was not directly bound by the Charter. Following a request from law enforcement, it can transfer information concerning the appellant to another third party without their consent, so long as it respects the measures put in place[45]. Although disclosures must comply with statutory limitations, these protections are often less strict than constitutional standards. As a result, law enforcement can indirectly obtain

[39] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982 [Schedule B to the Canada Act 1982, 1982, c. 11 (U.K.)], art. 8, p 24(2).
[40] *R.* v. *Grant*, 2009 SCC 32.
[41] *R.* v. *Spencer*, 2014 SCC 43.
[42] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982 [Schedule B to the Canada Act 1982, 1982, c. 11 (U.K.)], art. 8.
[43] *R.* v. *Spencer*, 2014 SCC 43, Criminal Code, R.S.C. 1985, c. C-46, art. 487.
[44] Criminal Code, R.S.C. 1985, c. C-46, art. 487.1.
[45] Act respecting the protection of personal information in the private sector, C.Q.L.R., c. P-39.1, art. 18.4.

sensitive information, such as data linked to an IP address, through the actors who fall outside the Charter's reach. This creates a gap in accountability, where personal information can circulate between private entities and the police without the person's knowledge or consent, and without the proper procedural guarantees that would normally apply if the State sought out the information directly.

3.2. Privacy and data protection in Europe

Secondly, similar challenges arise under the ECHR and the GDPR. The *Breyer* case illustrates how IP-address-based investigations intersect with privacy rights, portraying tensions between the State's investigatory powers and individuals' rights to informational privacy. European legal frameworks, while emphasizing proper data protection and proportionality, face issues with third-party actors, technological complexity, and the evolving nature of digital surveillance. These developments show that the challenges posed by IP address-based investigations are not unique to Canada, but reflect a global tension between privacy and law enforcement.

To continue, *Breyer* illustrates that European law recognizes IP addresses should be protected, as they may reveal private information. In fact, according to art. 8 of the ECHR, individuals are entitled to respect for private life, which includes digital communications[46]. Any interference with this right must be done with legal cause. Moreover, the GDPR classifies IP addresses as personal data, requiring that processing by ISPs respects principles of lawfulness, necessity, and proportionality. Despite these protections, *Breyer* exposes persistent challenges, similar to the ones in *Bykovets*. Even though the GDPR imposes obligations on data controllers, law enforcement can obtain personal data without direct consent, thus bypassing constitutional protections.

Additionally, the Directive is an attempt to better navigate the digital space. It requires telecommunication providers to retain metadata, including IP addresses, for periods ranging from six to twenty-four months to help in investigating, detecting, and prosecuting serious crimes, such as organised crime and terrorism. While it is meant to support law enforcement, this retention means that authorities would have access to personal data without the individual's consent, often indirectly through ISPs, similar to the concerns highlighted in *Breyer* and *Bykovets*. The European Court of Justice invalidated this Directive in *Digital Rights Ireland*

[46] Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 8.

and *Seitlinger and Others* (C-293/12 and C 594/12) because it disproportionately interfered with fundamental rights to privacy and data protection under art. 7, 8 and 52(1) of the ECHR.[47]

These examples demonstrate that while the law attempts to provide procedural requirements, the current measures are too broad to effectively regulate access to IP-related data. By allowing authorities to compel ISPs to disclose information, they create avenues for privacy intrusions that are not fully constrained by existing protections. Consequently, despite the presence of statutory and constitutional safeguards, current legal regimes remain insufficient to fully guarantee fundamental rights in the rapidly evolving digital environment.

CONCLUSIONS

To conclude, the realities of modern digital infrastructure reveal that existing legal protections are not equipped to properly regulate IP-address-based investigations. As cybercrime evolves, the need for effective enforcement is undeniable, but it cannot justify the erosion of privacy rights. Cases like *Bykovets* and *Breyer* depict how IP addresses are often dismissed as mere technical identifiers. In reality, they can uncover an individual's identity, behaviour, and overall digital habits. However, their ability to reveal such data relies on a fragmented chain of actors, from ISPs to third-parties, whose roles complicate the ability to protect privacy. This creates a paradox, where a person may feel compelled to limit online activity to avoid authorities intruding into their private life.

Both the Canadian and European legal frameworks, such as the Charter, the Criminal Code, the ECHR, the GDPR, and the Directive attempt to regulate the State's access to such data. *Bykovets* demonstrates how private actors hold crucial digital identifiers that fall outside the scope of constitutional scrutiny, while *Breyer* reveals how even dynamic IP addresses can be utilized to reconstruct intimate user profiles. The indirect access through third parties and broad measures indicates that the legal system is not adapted to the realities of contemporary surveillance.

This is why both domestic and international legal systems must evolve toward clearer, more technologically informed protections. Ideally, ones that recognize the intrinsic sensitivity of IP-address-based information and resist the normalization of digital intrusions. Nonetheless, accessibility and anonymity are essential concepts in a free and democratic society, but they

[47] *Digital Rights Ireland* and *Seitlinger and Others* (C-293/12 and C 594/12); Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 7, art. 8, art. 52(1).

also facilitate certain crimes, creating challenges for law enforcement. No matter how difficult strengthening privacy in the digital era may be, it is a necessary condition in order to maintain trust and safety in an increasingly interconnected world.

BIBLIOGRAPHY

I. Doctrine

1. D. Gold, « Applying Section 8 in the Digital World: Seizures and Searches », document prepared for the 7th Annual Six-Minute Criminal Defence Lawyer (9 juin 2007), p 3.

II. Specialized articles and studies

1. Kamara, I., & De Hert, P. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*. Brussels Privacy Hub Working Paper, Vol. 4, No.12 (Brussels, 2018).

III. Sources in electronic format

1. Amazon Web Services, Inc., « What's the Difference Between HTTP et HTTPS? », 2024, available at: https://aws.amazon.com/compare/the-difference-between-https-and-http/.
2. BPP Human Rights Unit. *Article 8 and the "reasonable expectation of privacy test."* BPP Human Rights Law Blog, 2021, available at: https://bpphumanrightsunit.wordpress.com/2021/02/24/article-8-and-the-reasonableexpectation-of-privacy-test/.
3. Brennan, D. *CJEU rules IP addresses may constitute personal data*. A&L Goodbody, 2016, available at: https://www.algoodbody.com/insights-publications/cjeu-rules-ip-addresses-may constitute-personal-data.
4. Đukanović, J. *Is IP address personal data?*. Zunic Law, Serbia, 2025, available at: https://zuniclaw.com/en/ip-address-personal-data/.
5. Wahl, T. *ECJ Ruled on Data Retention of IP Addresses in Piracy Cases*. Eucrim, Germany, 2024, available at: https://eucrim.eu/news/ecj-ruled-on-data-retention-of-ip-addresses-in-piracy cases/.

IV. Case law

1. *Breyer* v. *Germany*, 2020, 50001/12.
2. *Digital Rights Ireland* and *Seitlinger and Others* (C-293/12 and C 594/12). *R.* v. *Ahmad*, 2020 SCC 11.
3. *R.* v. *Bykovets*, 2024 SCC 6.
4. *R.* v. *Grant*, 2009 SCC 32.
5. *R.* v. *Ramelson*, 2022 SCC 44.
6. *R.* v. *Spencer*, 2014 SCC 43.
7. *R.* v. *Vu*, 2013 SCC 60.

V.Legislation

1. Act respecting the protection of personal information in the private sector, C.Q.L.R., c. P 39.1, art. 18.4.
2. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982 [Schedule

B to the Canada Act 1982, 1982, c. 11 (U.K.)], art. 8, p 24(2).
3. Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 7, art. 8, art. 10, art. 52(1).
4. Criminal Code, R.S.C. 1985, c. C-46, art. 487.
5. Criminal Code, R.S.C. 1985, c. C-46, art. 487.1.
6. Data Retention Directive (2006/24/EC).
7. Personal Information Protection and Electronic Documents Act, S.C.2000, c. 5. Privacy Act, R.S.C. 1985, ch. P-21.
8. Regulation (EU) 2016/679 (General Data Protection Regulation), art. 4(1).